LEVIN LAW, P.A.
Brian Levin (*admitted by PHV*)
brian@levinlawpa.com
Brandon T. Grzandziel (*pro hac vice* to be filed)
brandon@levinlawpa.com
2665 South Bayshore Drive, PH2B
Miami, Florida 33133
Telephone 305-539-0593

Jacob Polin (SBN 311203)
jacob@levinlawpa.com
344 20th Street
Oakland, CA 94612
Telephone: (305) 402-9050

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Attorneys for Plaintiffs & the Proposed Classes

[*Additional Counsel for Plaintiffs Listed on Signature Page*]

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE: OTTER.AI PRIVACY LITIGATION

Case No. 5:25-cv-06911-EKL

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL ENCLOSED

INTRODUCTION

1. Defendant Otter.ai, Inc. ("Otter") has developed and provides to the public an artificial intelligence-powered meeting assistant called Otter Notetaker.

2. Otter Notetaker engages in real-time transcription of Google Meet, Zoom, and Microsoft Teams meetings for Otter accountholders and other users.

3. Publicly, Otter promises privacy; it says it "recognize[s] your conversations may contain some of your most sensitive and confidential information" and "believe[s]

transparency is important to all meeting participants," and "[t]hat's why we are committed to keeping your information private and secure."[1]

4. Behind these promises, Otter spies. Otter Notetaker slips surreptitiously into meetings as a silent participant. It records audio. It takes screenshots of conversations, along with audio recordings, and stores everything without the participants' knowledge or consent.

5. By virtue of providing the Otter Notetaker service, Otter accesses and records the contents of private conversations between Otter accountholders who use the Otter Notetaker and meeting participants who do not subscribe to Otter's services.

6. Consequently, Otter's surreptitious surveillance extends far beyond its own user base. When an Otter accountholder connects their calendar, Otter silently, and automatically, joins every meeting and begins recording and transcribing the conversation, as well as taking screenshots of the video call.

7. No one is asked or warned of what Otter does. Most participants never know. They only learn later, when partial transcripts or screenshots appear in their inbox – in an email *after* the meeting is concluded.

8. Otter Notetaker hides in plain sight, often indistinguishable from a real person in the room. It appears as the user's notetaker—for instance, "Anna's Notetaker (Otter.ai)" —and provides no visual or auditory notice to other meeting participants that the meeting is being recorded in real time, transcribed, and stored on Otter's servers for its own future use, including advertising and marketing, training of their AI models, development/improvement of their services, and other purposes.

9. As a result, Otter captures hundreds of thousands, if not millions, of participants without their informed consent. Confidential work meetings, recruiting interviews, legal strategy sessions, medical appointments, support groups, religious

[1] Otter, *Privacy & Security*, https://otter.ai/privacy-security (last visited Nov. 19, 2025).

meetings – the Otter Notetaker records them all.

10. Otter also collects names, emails, and contact details from platforms like Zoom, Microsoft Teams, Google calendar, and Outlook calendar, and links those details with the recorded transcripts, capable of identifying specific speakers to specific words at specific times.

11. Equally egregious, when in use, the Otter Notetaker creates a voiceprint associated with each speaker it records. These voiceprints are what Otter uses to create a transcript of the meeting. And it stores each voiceprint so that, in future meetings, Otter can identify the same individuals and transcribe their conversations.

12. The voiceprints Otter collects are biometric data subject to the protection of the Illinois Biometric Information Privacy Act ("BIPA").[2] And for good reason. Voiceprints require protection because they are often used to authenticate individuals' identities when those individuals seek access to restricted personal or financial information.

13. Thus, individuals whose voiceprints are stolen or compromised are at increased risk of identity theft and fraud. Accordingly, BIPA requires that private entities notify, and obtain consent from, individuals before collecting their voiceprints.

14. Crucially, Otter does not obtain prior consent, express or otherwise, of persons who attend meetings where the Otter Notetaker is enabled, prior to Otter recording, accessing, reading, and learning the contents of conversations between Otter accountholders and other meeting participants (or before collecting biometric data).

15. Moreover, Otter completely fails to disclose to those who do set up Otter to run on virtual meetings but who are recorded by the Otter Notetaker that their conversations are being used to train Otter Notetaker's automatic speech recognition ("ASR") and machine learning models, and in turn, to financially benefit Otter's business.

[2] Herein, the term "biometric data" refers collectively to biometric information and biometric identifiers, as defined within BIPA.

16. Likewise, Otter automatically collects voiceprints from meeting participants without notifying them that it is collecting their biometric information, much less obtaining their consent to, or a required written release for, that collection.

17. These BIPA violations are reckless and intentional as Otter's website shows that it canvassed state-by-state data privacy laws (and even international privacy laws) before releasing the Otter Notetaker. While Otter claims to have taken steps to ensure its software complies with many of these laws, it has made no effort to comply with BIPA, even though its investigation of data privacy laws must have apprised Otter of BIPA's requirements.

18. Otter's actions—taken without user consent and for its own financial benefit—resulted in severe privacy violations for thousands, if not millions, of individuals across the United States including, but certainly not limited to, the Plaintiffs Justin Brewer ("Plaintiff Brewer"), Chaka Theus ("Plaintiff Theus"), Emily Ryan ("Plaintiff Ryan"), Jasper Pierson Walker ("Plaintiff Jasper Walker"), Michael Walker ("Plaintiff Michael Walker"), Nadine Winston ("Plaintiff Winston"), and Riley Dolan ("Plaintiff Dolan") (collectively, the "Plaintiffs").

19. Through its use of the Otter Notetaker, Otter has failed to comply with federal, California, Illinois, and Washington law. Accordingly, Plaintiffs, on behalf of themselves and a class of similarly situated individuals, assert individual and representative claims for violation of the following statutes: (i) the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. § 2510, *et seq.*; (ii) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; (iii) the California Invasion of Privacy Act ("CIPA") Cal. Penal Code §§ 631, 632, 635, and 638.50-.56; (iv) California's Comprehensive Computer Data and Fraud Access Act ("CDAFA"), Cal. Penal Code § 502, *et seq.*; (v) California's statutory prohibition against larceny and the receipt of stolen property, Cal. Penal Code § 496(a) and (c); (vi) the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*; (vii) Illinois' BIPA, 740 ILCS §§ 14/15(a)

and 14/15(b); and (viii) Washington's Wiretapping Law, Wash. Rev. Code §§ 9.73.030, *et seq*. Plaintiffs also assert individual and representative claims for the common law torts of intrusion upon seclusion, trespass against chattels, and conversion as well as for California's constitutional prohibition against invasion of privacy and a request for a Declaratory Judgment.

PARTIES

20. Plaintiff Brewer is a natural person and citizen of California who resides in San Jacinto, California, where he intends to remain.

21. Plaintiff Theus is a natural person and citizen of California who resides in Los Angeles, California, where she intends to remain.

22. Plaintiff Ryan is a natural person and citizen of California who resides in Irvine, California, where she intends to remain.

23. Plaintiff Jasper Walker is a natural person and citizen of Illinois who resides in Chicago, Illinois, where she intends to remain.

24. Plaintiff Michael Walker is a natural person and citizen of Illinois who resides in Chicago, Illinois, where he intends to remain.

25. Plaintiff Nadine Winston is a natural person and citizen of Illinois who resides in Northbrook, Illinois, where she intends to remain.

26. Plaintiff Riley Dolan is a natural person and citizen of Washington who resides in Seattle, Washington, where he intends to remain.

27. Defendant Otter is a global technology company that provides AI-powered meeting transcription, voice recording, and productivity software for independent professionals and businesses. Otter is incorporated under Delaware law. Its principal place of business is located at 800 W. El Camino Real, Suite 170 in Mountain View, California 94040.

JURISDICTION & VENUE

28. This Court has personal jurisdiction over Otter because its principal place of

business is in California.

29. On information and good faith belief, Otter's decisions concerning use of its Otter Notetaker software to intercept Class members' communications and voiceprints and train its ASR and machine learning tools emanated from its California headquarters.

30. All Class members' claims arise from, and are closely related to, Otter's contacts with California. Thus, it is also fair and reasonable for this Court to exercise jurisdiction over Otter.

31. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). At least one member of the proposed Class is a citizen of a state different from that of Otter; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members, and none of the exceptions under the subsection apply to this action.

32. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges claims arising under federal law—specifically, under the ECPA and CFAA. Moreover, the Court may exercise supplemental jurisdiction over the California, Illinois, and Washington state law claims contained in this Complaint pursuant to 28 U.S.C. § 1367.

33. Venue is proper in the Northern District of California because Otter's principal place of business is in Mountain View and a substantial part of the events or omissions giving rise to the Plaintiffs' claims occurred in this district.

FACTUAL ALLEGATIONS

A. Otter's Nonconsensual Interception and Use of Plaintiffs' and Class Members' Communications

34. Otter is a rapidly growing technology company, offering a transcription and productivity platform that integrates with various widely used professional communication services, including Zoom, Google, and Microsoft Teams.

35. This is not surprising given that in the wake of the COVID-19 pandemic, the

American workplace underwent a profound transformation, evolving into a permanent shift, with millions of professionals now working entirely online. As a result, meetings once conducted face-to-face in conference rooms and coffee shops, are now hosted via Zoom, Microsoft Teams, Google Meets, and other video conferencing platforms. By 2023, over 35% of full-time employees in the United States regularly worked remotely, and an even greater percentage participated in hybrid work environments.

36. Since 2016, Otter has grown rapidly, processing over 1 billion meetings for 25 million global users ranging from individuals to startups and Fortune 500 companies.[3]

37. Otter has become one of the most used virtual note-takers, marketing itself as the "leading AI Meeting agent."[4]

38. In March of 2025, the company surpassed $100 million in annual recurring revenue ("ARR"), an exceptional figure for a company of Otter's size.[5]

39. Much of Otter's growth is attributable to its AI-powered meeting assistant, the Otter Notetaker. The Otter Notetaker, whose software and functionality is also part of a broader and enhanced AI transcription service called OtterPilot, is available to Otter accountholders.

40. For Otter accountholders, the Otter Notetaker automatically joins scheduled Google Meet, Zoom, and Microsoft Teams meetings through synced calendar events to provide real-time transcription.[6] However, many Otter accountholders do not realize that

---

[3] *Otter.ai Breaks $100M ARR Barrier and Transforms Business Meetings Launching Industry-First AI Meeting Agent Suite*, OTTER (March 25, 2025), https://otter.ai/blog/otter-ai-breaks-100m-arr-barrier-and-transforms-business-meetings-launching-industry-first-ai-meeting-agent-suite#:~:text=With%20over%2025%20million%20global,agentic%20AI%2C%20but%20defining%20it (last accessed August 12, 2025).

[4] *Id.*

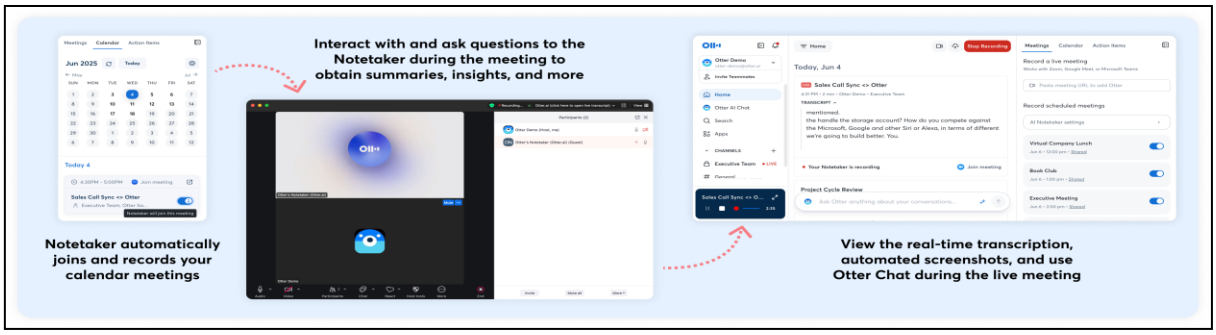
[5] *See*, *supra*, n.1.

[6] *Stop Otter Notetaker from automatically joining your meetings*, OTTER (July 2025), https://help.otter.ai/hc/en-us/articles/12906714508823-Stop-Otter-Notetaker-from-

Otter Notetaker will then join and record every meeting set on their calendars.

41. In doing so, it transmits data directly to Otter in real time for processing and transcription purposes.[7] (*See* Image 1, below).

Image 1



42. Thus, the Otter Notetaker is not a tool used solely by the accountholder to record others. Instead, the Otter Notetaker is a tool used by Otter itself—a separate and distinct third-party entity from its accountholders and other parties to the conversation—to record and transcribe conversations to which it is not a party.

43. Otter does not notify the participants that it intends to record the entire meeting, and often, depending on the platform they are using, participants might not be able to remove Otter Notetaker from the meeting.

44. As a result, Otter Notetaker joins the meeting without obtaining the affirmative consent from any meeting participant. It could also join meetings on which the Otter accountholder is not present at all.

45. Moreover, while Otter has the ability to send pre-meeting notification that it will join and automatically record all participants during the call unless they exclude the notetaker from the meeting, it does not do so.

46. Other companies and platforms alert participants if someone starts

---

automatically-joining-your-meetings.

[7] *Otter Notetaker Overview*, OTTER, https://help.otter.ai/hc/en-us/articles/4425393298327-Otter-Notetaker-Overview (last accessed August 12, 2025).

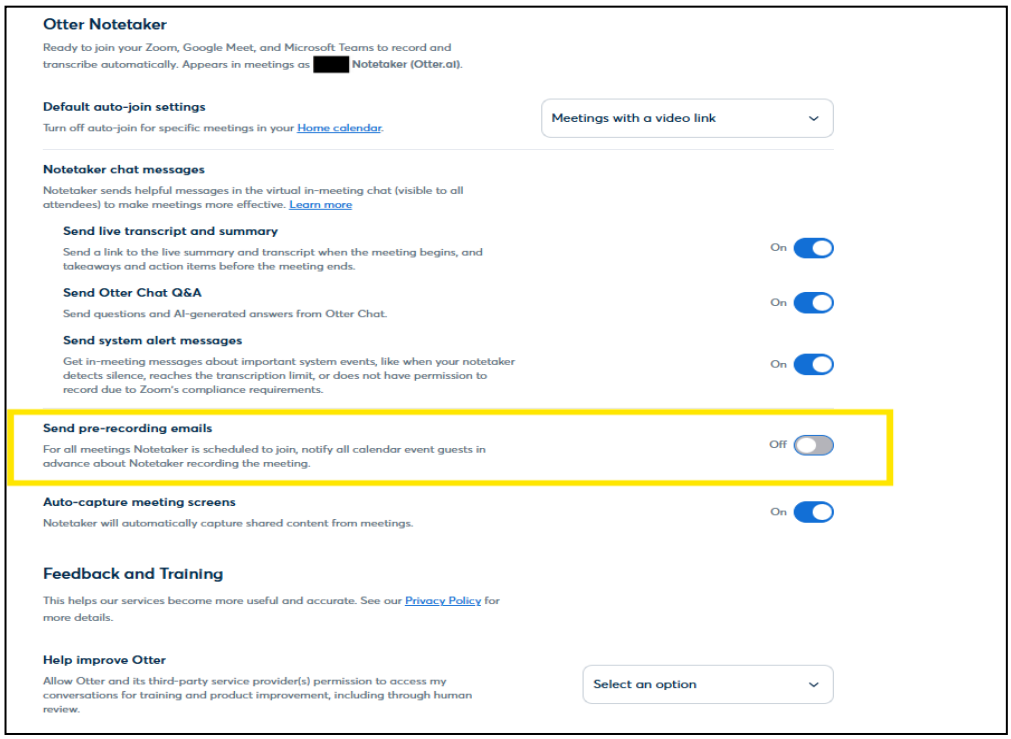
recording. For instance, Zoom and Microsoft Teams prominently announce that a recording has started, automatically muting and turning off cameras for all participants until they consent to the recording/use of their video. Otter could notify users as well by sending email in advance of the meeting notifying all participants that it will record them, and by playing a pre-recorded voice message announcing its recording and displaying the same message in the chat before it starts the recording. Otter chooses not to do that.

47. Instead, Otter accountholders must toggle this setting "On" for it to apply to pre-scheduled meetings.[8]

48. Below is a screenshot demonstrating that when default account settings are used, the pre-meeting email notification setting is turned "Off." (*See* Image 3, below).

[8] *Manage your Otter Notetaker Settings*, OTTER, https://help.otter.ai/hc/en-us/articles/13675989227543-Manage-your-Otter-Notetaker-settings (referring to toggling the pre-meeting notification setting "on") (last accessed August 12, 2025); *Enforce pre-meeting recording notifications*, OTTER, https://help.otter.ai/hc/en-us/articles/13353091821591-Enforce-pre-meeting-recording-notifications (indicating that pre-meeting recording notifications must be "turned on" by businesses who subscribe to Otter's Enterprise plan) (last accessed August 12, 2025).

Image 3



49. Furthermore, when Otter Notetaker joins a meeting, it does not provide meeting participants with reliable or automatic visual or auditory alerts to meeting participants indicating that the meeting is being recorded or transcribed, let alone notice regarding the real-time transmission of their data to Otter or the way in which the company ultimately uses their data.

50. When Otter Notetaker joins a meeting, the application enters the meeting as a silent participant and begins recording audio, transcribing contents in real time while sending and storing the recordings, and capturing and sending data in real time to its servers. Otter does not obtain consent from non-accountholder meeting attendees. The participants on the call have no way of knowing that they are being recorded.

51. Often, the Otter Notetaker will not disclose its presence to meeting attendees at all.

52. Occasionally, if someone expressly inquires in the chat or asks a question about Otter—typically well into the conversation or at the very least after the conversation

had started and they had been recorded without notice or consent, Otter Notetaker will post a reply message in the chat, introduce itself as an "AI assistant" that is helping the designated Otter accountholder "take notes for this meeting." However, it does not disclose that it has been recording the entire conversation, and transmitting the conversation to its servers in real-time. The meeting participants who join via phone are not able to see the posted message at all (if it has been posted).

53. With the message that appears after someone inquires about Otter, Otter will also include a link to view the meeting notes, which prompts non-accountholders to sign up for Otter to view, an option that many do not select. Only if they create an account (after they had already been recorded without notice or consent) and view the transcript do they learn that their conversations have been recorded.

54. At this point, Otter has already began taking screenshots, recording audio, timestamping statements, labeling speakers, analyzing voiceprints, and analyzing the obtained data.

55. Most of the time, Otter Notetaker appears and disappears as a silent participant with no message at all.

56. Even if these rare disclosures are made, participants are often mid-conversation and do not realize what is happening and do not have time to investigate Otter's automated message that only suggests note taking – not recording, transcribing, and storing the entirety of the conversation.

57. Most participants do not use the provided link inconspicuously suggesting it is to follow "notes" while actively engaged in a meeting and unable to create the account, unaware that Otter has been recording their private discussions from the moment it joined.

B. Otter's Well-Documented Failures to Provide Sufficient Notice and Obtain Consent from Meeting Participants

58. As a result of Otter's default settings and lack of notice, even Otter's

accountholders are frequently unaware that the Otter Notetaker is transcribing and sending meeting data, while non-accountholder participants receive no notice at all and are therefore entirely unaware until such data has already been shared.

59. For example, around February 2023, Otter originally introduced the Otter Notetaker feature with a pop-up setup page which included a toggle automatically set to share meeting notes with meeting attendees.

60. Many Otter accountholders clicked on "Enable Otter Assistant," without realizing that they had given permission to Otter to attend all their meetings (even when accountholders are not present), record the entire meeting, and share transcribed meeting notes with non-accountholder attendees (regardless of their own attendance).[9]

61. Automatically enabling this feature for all accountholders, and without individual consent, was disastrous.

62. In a Reddit post, one Otter accountholder described a humiliating incident in which Otter automatically joined a job interview without their knowledge or permission. During the interview, an interviewer questioned whether the meeting was being recorded, the accountholder denied that it was, genuinely believing that to be true.

63. The accountholder was mortified to later discover that Otter had in fact recorded and transcribed the meeting, with notes distributed to all participants. Feeling frustrated he wrote: "Otter AI is seriously intrusive and I have no idea who now has access to a private meeting that I ensured (sic) all was NOT being recorded… This company Otter AI should be sued for the intrusive and devious nature it presents as well as privacy and security risks." The user concluded, "Needless to say – I will not get this job because Otter AI made me look like a liar and a fool! Unbelievable!"[10] (See Image 4, below).

---

[9] Barbara Krasnoff, *How to keep Otter from automatically recording your meetings*, OTTER (April 13, 2023), https://www.theverge.com/23660324/otter-record-transcribe-how-to-stop.

[10] u/Specialist-Maize-957, Comment to *Do not join Otter.Ai unless you want your whole company spammed*, REDDIT (July 17, 2025),

Image 4

64. In another instance, researcher and engineer Alex Bilzerian joined a Zoom meeting with a venture-capital firm and the Otter Notetaker was used to record the call. After the meeting, Otter automatically emailed Bilzerian and other participants a transcript of the call, which included "hours of their private conversations afterward, where they discussed intimate, confidential details about their business." Bilzerian described that, after he had exited the call, investors discussed their firm's "strategic failures and cooked metrics." After notifying the investors that they had inadvertently shared confidential details about their firm, Bilzerian ultimately decided to terminate his potential deal with them.[11]

65. Otter accountholders have also reported that even after attempting to disable Otter Notetaker's automatic join feature, Otter Notetaker continued to join meetings without any further action by the accountholder, and often without their knowledge. This has resulted in Otter Notetaker repeatedly appearing in private meetings, even after accountholders have attempted to disable it, and continue to record participants without consent.

---

https://www.reddit.com/r/projectmanagement/comments/1j0cfei/do_not_join_Otter.ai_unless_you_want_your_whole/.

[11] Brooke Kato, *AI is spying on your workplace gossip and secrets — and sharing them afterward,* NEW YORK POST (Oct. 4, 2024), https://nypost.com/2024/10/04/tech/ai-is-spying-on-your-workplace-gossip-and-secrets-and-sharing-them-afterward/.

66. For example, an Otter accountholder posted online that they "carefully opted out of" an Otter update that would enable Otter Notetaker to automatically join their meetings through their Google Calendar. Yet, they explained, "the [Otter.ai] bot proceeded to join two confidential meetings on my behalf and record the whole thing, then email every member an absurd, inaccurate 'outline' after." The user was extremely frustrated and felt "completely abused." They warned fellow users that they "opened a support ticket with screenshots [with Otter]," but, according to Twitter, Otter was neglecting to review any tickets from free users.[12] (*See* Image 5, below).

Image 5

C. Otter Trains Its Automatic Speech Recognition Model on User Conversations and Uses Personal Information It Receives from Meeting Attendees for Its Own Financial Benefit

67. Otter Notetaker's ability to accurately transcribe conversations depends upon its automatic speech recognition ("ASR") and machine learning models.

68. An ASR is an AI technology, often a machine learning algorithm, that converts spoken language into written text.

69. Otter has stated explicitly that it trains its AI models on recordings and transcriptions made using the Otter Notetaker.

---

[12] *arcticfox*, *Tell HN: Otter.ai bot recording meetings without consent*, HACKER NEWS (Sept. 7, 2022), https://news.ycombinator.com/item?id=32751071.

70. As part of its Privacy Policy, Otter states the following: "We train our proprietary artificial intelligence on de-identified audio recordings. We also train our technology on transcriptions to provide more accurate services, which may contain Personal Information. We obtain explicit permission (e.g. when you rate the transcript quality and check the box to give Otter.ai and its third-party service provider(s) permission to access the conversation for training and product improvement purposes) for manual review of specific audio recordings to further refine our model training data."[13]

71. As indicated by Otter's Privacy Policy, Otter does not seek the consent of meeting participants, besides the Otter accountholder, for using audio recordings or conversation transcriptions to train its ASR and machine learning models.

72. This audio recording data Otter obtains often contains the sensitive personal information of unsuspecting third parties, yet is stored and processed without obtaining their informed consent.

73. As part of its Privacy Policy, Otter implores its accountholders to "please make sure [they] have the necessary permissions from . . . co-workers, friends or other third parties before sharing Personal Information" in the event of an audio recording.[14]

74. In effect, Otter tries to shift responsibility, outsourcing its legal obligations to its accountholders, rather than seeking permission and consent from the individuals Otter records, as required by law.

75. Burying these requirements inside a dense privacy policy that Otter knows consumers do not read is not a meaningful disclosure of its illegal practices – even with respect to the accountholders. Otter has a duty to obtain consent under the applicable recording laws (as discussed below), and it cannot shift such responsibility by placing it in

[13] *Privacy Policy*, OTTER (September 1, 2024), https://otter.ai/privacy-policy (last accessed August 12, 2025).

[14] *Id.*

fine print of its privacy policy. The accountholders never see this disclosure, and often do not know that Otter is joining meetings again and again, including after the accountholders take steps to prevent Otter from joining the calls.

76. This practice allows Otter to harvest and use intimate conversational data and use it for its own purposes – including training of their AI systems, while attempting to insulate itself from accountability for the harm it creates by design.

77. And despite Otter's claim to "de-identify" audio recordings for AI training purposes, Otter provides the public no description of what this de-identification process entails. More importantly, the voiceprints it uses are biometric data. Even if supposed identifiers are purportedly stripped, the unique fingerprint with can be re-identified and matched with alarming accuracy. Once the voiceprints are used for AI training, the biometric data is not stripped nor can it be blurred out like a face in a video. Furthermore, the context/natures of conversations combined with voices identify people not purely on the email/name to which it is attached. Meetings contain highly specific details: company projects, internal conversations, use of names connected to voices, references to individual's professional and/or personal roles, and more. Even if explicit identifiers are removed, the voice recording of the meeting contains enough information to narrow speakers. What's more is that once something is used in the training of models, that information becomes embedded in system's behavior, and can be leaked in various forms. Therefore, even if Otter does "de-identify" some information, by feeding the meeting recordings into its machines, it does not and cannot truly anonymize the speaker information. Perhaps for this very reason, Otter does not describe this process as "anonymization," reflecting an implicit recognition that true anonymity cannot be achieved here.

78. Therefore, Otter's deidentification process does not remove confidential information or guarantee speaker anonymity.

79. Scientific research into de-identification of information used to train machine

learning models has revealed that even sophisticated de-identification procedures are unreliable.[15]

80. The inadequacy of de-identification for conversational data is compounded by Otter's policy of retaining data for an indefinite period. As stated in Otter's Privacy Policy, "Otter.ai stores all Personal Information for as long as necessary to fulfill the purposes set out in this Policy, or for as long as we are required to do so by law in order to comply with a regulatory obligation."[16]

81. Taken together, what Otter has done is use its Otter Notetaker meeting assistant to record, transcribe, and utilize the contents of conversations without Class members' informed consent.

82. Otter designed the Otter Notetaker to record and transcribe real-time virtual meetings and purposefully intended for the data obtained to train its ASR and machine learning models.

83. As such, when Otter provided the Otter Notetaker service to its accountholders, Otter understood and therefore intended to record the communications of the Class members without their consent.

84. This purpose and intention is exemplified by the fact that Otter does not engage in best industry practices. For example, a rival company, Read.ai, permits any conversation participant, including those who do not use Read.ai, to stop recording during a meeting.[17]

---

[15] *See, e.g.*, Atiquer Sakar, *et al.*, De-identification is not enough: a comparison between two de-identified and synthetic clinical notes, 14 Sci. Rep. 29699, 5 (2024) ("We trained a machine learning classifier with de-identified clinical notes. We mounted a membership inference attack on the classifier and found the attack quite successful. This finding has far-reaching privacy implications for membership-sensitive models that use clinical notes in their training.").

[16] *Id.*

[17] *How do I remove or stop Read from joining meetings?*, READ,

85. The failure of Otter to include such functionality for its own transcription services is thus indicative of its intent to record conversations in the absence of participants' informed consent.

86. What is more, Otter exploits the private, identifying and recorded information of meeting participants to send automated emails to non-accountholder attendees, often including transcripts and summaries, to encourage them to sign up for Otter's services.

87. Beyond spamming non-accountholders with Otter's promotional emails, Otter uses the recordings it obtains for a variety of its own purposes including (as previously mentioned) improving its services and training its ASR, but also processing job applications (if someone were to apply to work for Otter), social network support (such as sending messages purportedly on behalf of users to social networks), contracting vendors, research, and even sharing the collected data with other third parties such as analytics providers, advertisers, vendors, social networks, and more.

88. In addition to secretly recording and transcribing non-user participants' voices and statements, Otter collects and stores identifying information about these individuals, including their names and email addresses, by extracting data from the Otter accountholder's calendar invites and meeting metadata, often without the knowledge or consent of the Otter accountholder, let alone all meeting participants.

89. At first, Otter emails all invitees to the call after the call is concluded, inviting them to access the notes of the call. These emails are deceptive, appearing simply as shared meeting notes. Non-accountholders who want to access these notes, that appear to have been shared by their colleagues, open the link in their emails to discover that they must sign up for Otter to access the notes.

---

https://support.read.ai/hc/en-us/articles/23222131547795-How-do-I-remove-or-stop-Read-from-joining-meetings (last accessed August 12, 2025).

90. Unfortunately, those individuals who try to access notes and are forced to create an account are often automatically enrolled in the service that allows Otter to join the calls that appear on their calendar and initiate the non-consensual recordings. Only if these users create the account can they discover that they had been illegally recorded.

91. Previously, Otter's onboarding process included calendar syncing as a default setting and did not offer users the option to customize what data or permissions would be shared throughout the set-up process.

92. Recently, Otter began allowing new users to select calendar preferences at signup, but the default options remained the same—to share the entire calendar and contact information of the participants.

93. Even with the new set up, the platform continues to join and record meetings without notifying or obtaining consent from non-user attendees.

94. As one of the Otter's accountholders accurately explained in complaining about Otter's behavior: "[Otter's] user acquisition approach is basically to spread like a virus…Most users have no idea [they have granted Otter access to their meetings], they're just there for the meeting notes (at the prompting of a trusted colleague/earlier victim)."[18]

95. When another user replied that the situation seemed problematic, the original user described Otter's software as a "privacy and security nightmare."[19]

96. Otter uses the collected data to continue bombarding the participants with commercial emails, enticing them to sign up for its services – without the users' permission, knowledge, or consent. Otter uses the account holders' names to indicate that the email was sent on their behalf -when in reality – it never was. The Otter accountholders don't want to bombard their friends, colleagues, or family with spam; they

[18] u/Neither-State-211, Post titled *Otter.ai rant*, REDDIT (January 2025), https://www.reddit.com/r/sysadmin/comments/1i3rsds/Otter.ai_rant/.

[19] *Id.*

do not even know the emails are sent on their behalf by Otter, and solely to Otter's commercial benefit.

97. Overall, Otter takes, processes, stores, and profits from the data of non-accountholders even though these individuals have never agreed to Otter's Terms of Service or Privacy Policy.

98. Otter thus benefits from obtaining as much data as possible since it uses such data to improve its software for its own commercial purposes regardless of source or lack of consent.

99. Otter cannot rely on users' "consent" to justify its surveillance of non-users.

100. Not only is Otter aware that many of its accountholders do not realize that it's recording and intercepting all their calls as they have repeatedly and openly complained, but also, Otter subscribers have no authority to waive the privacy rights of other meeting participants, nor could they meaningfully obtain informed consent when Otter itself conceals the scope of its data practices.

101. Accountholders do not know the full extent of Otter's uses of private information – such as training AI models or fueling targeted marketing. Consent requires knowledge and transparency.

102. In short, the subscribing users lack the full picture, making it impossible for them to secure lawful consent on behalf of anyone else.

D. Plaintiffs' and Class members' data is valuable

103. Plaintiffs' and Class members' data has value, and Otter harmed Plaintiffs and the Class members by not compensating them for the value of their data and in turn decreasing its value.

104. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

105. The robust market for Internet user data has been analogized to the "oil" of

the tech industry.[20] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[21] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

106. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[22]

107. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[23]

108. Another example of this is the Neon app, which pays users for recording their phone conversations, which are subsequently passed along to AI developers who use it to train their chatbots. Neon pays users 30 cents per minute when they speak with other Neon members and 15 cents per minute for speaking to a non-Neon user. In either case, only the Neon users' side of the conversation is shared, and users can earn up to $30 per

[20] *See The world's most valuable resource is no longer oil, but data*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Feb. 13, 2024).

[21] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Feb. 13, 2024).

[22] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV.L.REV. 2055, 2056-57 (2004).

[23] *See 10 Apps for Seling Your Data for* Cash, https://wallethacks.com/apps-for-selling-your-data/ (last visited Feb. 13, 2024).

day for their conversations.[24]

109. This shows the immense value that software and machine learning developers find in the data available in individual conversations that can be used for training their AI systems, and it is clear that Otter is obtaining significant value from these illicitly recorded conversations.

110. There are countless other examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

111. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

112. For example, a study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[25] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[26]

---

[24] Lance Whitney, *This app will pay you $30/day to record your phone calls for AI - but is it worth it?*, ZDNET (September 25, 2025), https://www.zdnet.com/article/this-app-will-pay-you-30day-to-record-your-phone-calls-for-ai-but-is-it-worth-it/ (last accessed November 26, 2025).

[25] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/ (last accessed Sept 25, 2023).

[26] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed Sept 25, 2023).

113. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[27]

114. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

115. Defendants surreptitiously collected and used Plaintiffs' and Class members' data, including the information gathered within their conversations and obtaining their voiceprints, in violation of Plaintiffs' and Class members' privacy interests.

E. Otter's Collection and Possession of Biometric Data Violates BIPA

116. To facilitate its transcription process, Otter relies on "cutting-edge voice recognition technology" which is aided by its ASR.[28]

117. This technology collects "speaker identification data" that consists of individuals' unique voiceprints ("Speaker Data").[29]

118. Otter then associates the Speaker Data with individuals' identities. This occurs in one of two ways. When one of Otter's clients uses the OtterPilot, it "automatically tag[s] speakers in real-time based on the participant names of Zoom meetings."[30] When one of Otter's clients/accountholders uses the basic Otter Notetaker without Pilot functionality, Otter will provide generic labels to each speaker (such as "Speaker 1" and "Speaker 2"), and the client then "tags" each speaker by manually typing in their name.

---

[27] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook (last accessed Sept 25, 2023).

[28] Simon Lau, *What is Otter AI?*, OTTER (March 24, 2024), https://web.archive.org/web/20240918135606/https://otter.ai/t/meeting-insights/what-is-otter-ai

[29] Otter Help, *Speaker Identification Overview*, OTTER, https://tinyurl.com/2sd6kumh.

[30] *Id.*

119. Tagging creates a "speaker identification profile" associated with the name and the Speaker Data.[31] Otter then retains the Speaker Data so that Otter "will be able to recognize that speaker in future conversations."[32] In those conversations, Otter automatically associates the Speaker Data with the speaker's identity for transcription purposes, which confirms that regardless of any purported "de-identification" process, Otter trains its AI systems on the voice recordings to subsequently identify speakers automatically.

120. Otter retains Speaker Data indefinitely.

121. An FAQ page on Otter's website states as follows: "Can I delete a speaker? No. You cannot delete a speaker at this time."[33]

122. Meeting participants who have their Speaker Data or voiceprints collected and stored indefinitely by Otter are thus unable to even easily discern that Otter is collecting and storing the biometric information, or ensure that it's deleted and not used for Otter's future commercial benefit.

123. Through the foregoing process, Otter collected and possessed Plaintiffs' Speaker Data and linked it to the Plaintiffs' names during the meetings in which Plaintiffs participated and also collected and possessed Speaker Data from members of the Illinois Subclass in numerous other meetings and conferences during the statutory limitations period applicable to this suit.

124. Otter did not obtain consent before collecting and possessing the biometric data, as Otter never informs anyone that their voiceprints or biometric data are being collected. Nor are they asked to execute a release authorizing the collection of their

---

[31] Otter Help, *Rematch a Speaker*, OTTER, https://help.otter.ai/hc/en-us/articles/21665876084119-Rematch-a-speaker.

[32] *See, supra*, n. 29.

[33] *See id.*

biometric data.

125. Prior to collecting the Plaintiffs' biometric data, Otter did not publish any publicly available, written policy concerning how and when it retains and destroys biometric data in compliance with BIPA. In fact, Otter's publicly available policies do not mention or discuss BIPA at all.

126. Otter's violations of BIPA were negligent, reckless, and/or intentional.

127. Illinois enacted BIPA in 2008. Since that time, numerous articles regarding the law's requirements have been published. Numerous lawsuits regarding the same have been filed and the requirements are well known. Due to these articles and lawsuits, Otter knew or should have known that its data collection practices violated the law.

128. This is especially so given that Otter apparently canvassed state, federal, and international data privacy laws in connection with the release of its Terms of Service ("Terms").

129. The Terms direct Otter's vendors to "comply with the obligations" of the "State Privacy Laws" defined within the Terms.[34] Otter lists State Privacy Laws to include the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.[35]

130. Yet Otter does not name BIPA even though it is clear, from elsewhere on its website, that Defendant has reviewed Illinois law. Its website provides a "state-by-state breakdown" of laws governing call recordings, which includes a section on Illinois.[36]

---

[34] *Terms of Service*, OTTER, https://otter.ai/terms-of-service (last visited November 7, 2025).

[35] *Id.*

[36] Simon Lau, *Is it Illegal to Record Someone Without Their Permission*, OTTER (Feb. 11, 2025), https://otter.ai/blog/is-it-illegal-to-record-someone-without-their-permission.

131. Otter also names international data privacy laws in its Terms. They include the European Union's General Data Protection Regulation and the United Kingdom's Data Protection Regulation and e-Privacy Directive.[37]

132. During its exhaustive search of domestic and foreign law, Otter must have (or should have) become acquainted with BIPA's requirements. Yet Otter nevertheless disregarded those requirements.

133. Otter's hesitance to comply with BIPA may be explained by the value that Otter derives from collecting and retaining biometric data. Otter relies on the dataset of voiceprints it collects to run Otter and to continue building and training its software.

134. As Otter puts it in a now-deleted page of its website: "Otter AI relies on cutting-edge voice recognition technology to provide its services. At the forefront of this technology is machine learning, where the system continuously improves its speech recognition capabilities based on a vast dataset of voices and accents."[38]

F. Representative Plaintiff Brewer's Experience

135. Plaintiff Brewer participated in a Zoom meeting in California on February 24, 2025, where the Otter Notetaker was used by a meeting participant to transcribe the conversation that transpired therein (the "Conversation").

136. Plaintiff Brewer was not and is not an Otter accountholder.

137. Plaintiff Brewer was not aware, nor did he have any reason to suspect that Otter would obtain, illegally record, and retain his conversational data and Speaker Data, storing Brewer's private conversations on its servers indefinitely.

---

[37] *See, supra*, n. 35.

[38] Simon Lau, *What is Otter AI?*, OTTER (March 24, 2024), https://web.archive.org/web/20240918135606/https://otter.ai/t/meeting-insights/what-is-otter-ai/.

138. Nor was Plaintiff Brewer informed that Otter would use his communications and Speaker Data to train its ASR and machine learning tools.

139. Through this process, Otter read and learned, in real time, the contents of Plaintiff Brewer's communications, and transmitted them simultaneously to its servers.

140. Otter did not procure Plaintiff Brewer's prior consent, express or otherwise, to have Otter eavesdrop, record, and use his communications and Speaker Data. Nor did Plaintiff Brewer give his prior consent, express or otherwise, to Otter to allow Otter to wiretap his communications or intercept his Speaker Data.

141. Further, Plaintiff Brewer never consented to Otter's use of his communications and Speaker Data to train its ASR and machine learning systems or indefinitely store his private communications and exploit them for commercial gain.

142. Plaintiff Brewer neither granted nor would have granted Otter consent to record his Conversation on Zoom or obtain his Speaker Data if he had been given the opportunity.

143. Plaintiff Brewer's private conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff' Brewer's express and informed consent. The intrusion is especially troubling given the sensitive nature of the discussion and Plaintiff Brewer's expectation of confidentiality.

144. Plaintiff Brewer felt frustrated, embarrassed, and stressed to learn that his conversation was recorded without his consent, and his information, voice, and conversation content remains in Otter's possession indefinitely for Otter's commercial use and training of its machines/technology.

145. Plaintiff Brewer has, therefore, had his privacy severely invaded and been exposed to the risk and harmful conditions created by Otter's violations of federal and California law alleged below.

G. Plaintiff Chaka Theus's Experience

146. Plaintiff Theus participated in a Zoom meeting in California in March 2025

where the Otter Notetaker was used by a meeting participant to transcribe the conversation that transpired therein.

147. Plaintiff Theus used Zoom to communicate with a medical professional, and thus, the call involved deeply personal and private medical information which Otter recorded, transcribed, and stored without her knowledge, permission, or consent.

148. Plaintiff Theus was not, and is not, an Otter accountholder.

149. Plaintiff Theus was not aware, nor did she have any reason to suspect that Otter, as opposed to the Otter accountholder, would obtain and retain her conversational data and Speaker Data.

150. Nor was Plaintiff Theus informed that Otter would use her communications and Speaker Data to train its ASR and machine learning tools.

151. Through this process, Otter read and learned, in real time, the contents of Plaintiff Theus's communications.

152. Otter did not procure Plaintiff Theus's prior consent, express or otherwise, to have Otter eavesdrop, record, and use her communications and Speaker Data. Nor did Plaintiff Theus give her prior consent, express or otherwise, to Otter to allow Otter to wiretap her communications or intercept her Speaker Data.

153. Further, Plaintiff Theus never consented to Otter's use of her communications and Speaker Data to train its ASR and machine learning systems or indefinitely store her private communications and Speaker Data and exploit them for commercial gain.

154. Plaintiff Theus neither granted nor would have granted Otter consent to record her conversation on Zoom or obtain her Speaker Data if she had been given the opportunity.

155. Plaintiff Theus's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff' Theus's express and informed consent. The intrusion is especially troubling given the sensitive

nature of the discussion and Plaintiff Theus's expectation of confidentiality.

156. Plaintiff Theus felt frustrated, embarrassed, and stressed to learn that her conversation was recorded without her consent, and her information, voice, and conversation content remains in Otter's possession indefinitely for Otter's commercial use and training of its machines/technology.

157. Plaintiff Theus has, therefore, had her privacy severely invaded and been exposed to the risk and harmful conditions created by Otter's violations of federal and California law alleged below.

H. Plaintiff Emily Ryan's Experience

158. Plaintiff Ryan participated in a Microsoft Teams meeting in California on or around January 2025 where the Otter Notetaker appeared as one of her co-worker's notetakers. Plaintiff Ryan had no reason to suspect that the conversation is being recorded.

159. Plaintiff Ryan used Microsoft Teams to communicate with her work colleague(s) regarding sensitive discussions, which Otter recorded, transcribed, and stored without her knowledge, permission, or consent.

160. To her knowledge, Plaintiff Ryan did not create an account with Otter.

161. Plaintiff Ryan was not aware, nor did she have any reason to suspect that Otter would obtain and retain her conversational data and Speaker Data.

162. Nor was Plaintiff Ryan informed that Otter would use her communications and Speaker Data to train its ASR and machine learning tools.

163. Through this process, Otter read and learned, in real time, the contents of Plaintiff Ryan's communications.

164. Otter did not procure Plaintiff Ryan's prior consent, express or otherwise, to have Otter eavesdrop, record, and use her communications and Speaker Data. Nor did Plaintiff Ryan give her prior consent, express or otherwise, to Otter to allow Otter to wiretap her communications or intercept her Speaker Data.

165. Further, Plaintiff Ryan never consented to Otter's use of her communications and Speaker Data to train its ASR and machine learning systems or indefinitely store her private communications and Speaker Data and exploit them for commercial gain.

166. Plaintiff Ryan neither granted nor would have granted Otter consent to record her conversation on Microsoft Teams or obtain her Speaker Data if she had been given the opportunity.

167. Plaintiff Ryan's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff' Ryan's express and informed consent. The intrusion is especially troubling given the sensitive nature of the discussion and Plaintiff Ryan's expectation of confidentiality.

168. Plaintiff Ryan felt frustrated, embarrassed, and stressed to learn that her conversation was recorded without her consent, and her information, voice, and conversation content remains in Otter's possession indefinitely for Otter's commercial use and training of its machines/technology.

169. Plaintiff Ryan has, therefore, had her privacy severely invaded and been exposed to the risk and harmful conditions created by Otter's violations of federal and California law alleged below.

I. Plaintiff Jasper Walker's Experience

170. Plaintiff Jasper Walker participated in Zoom meetings while in Chicago, Illinois on January 10, 2025 and May 19, 2025 where the Otter Notetaker was used to transcribe the conversations that transpired therein, and during which Otter collected the biometric data and Speaker Data of the participants.

171. During the meetings, Plaintiff Jasper Walker used Zoom to communicate with a financial professional, and thus, the meetings involved deeply personal and private financial information.

172. Plaintiff Jasper Walker was not and is not an Otter accountholder.

173. Plaintiff Jasper Walker was not aware, nor did she have any reason to

suspect, that Otter would obtain and retain her biometric data and Speaker Data.

174. Nor was Plaintiff Jasper Walker informed that Otter would use her communications and Speaker Data to train its ASR and machine learning tools.

175. Through this process, Otter read and learned, in real time, the content of Plaintiff Jasper Walker's communications.

176. Otter did not procure Plaintiff Jasper Walker's prior consent, express or otherwise, to have Otter record and use her biometric data or Speaker Data. Nor did Plaintiff Jasper Walker give her prior consent, express or otherwise, to Otter to allow Otter to intercept her biometric data or Speaker Data.

177. Further, Plaintiff Jasper Walker never consented to Otter's use of her communications to train its ASR and machine learning systems or indefinitely store her private communications and Speaker Data and exploit them for commercial gain.

178. During the above-listed Zoom meetings, Otter captured Plaintiff Jasper Walker's voiceprint and voiceprints of other attendees, and it created a transcript of the conversations using the same.

179. Otter did so without first informing Plaintiff Jasper Walker that it was collecting her biometric data and without first obtaining, from her, a written release for the collection of that data.

180. Plaintiff Jasper Walker neither granted nor would have granted Otter consent to obtain her biometric data or Speaker Data if she had been given the opportunity.

181. Plaintiff Jasper Walker's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff Jasper Walker's express and informed consent. The intrusion is especially troubling given the sensitive nature of the discussion and Plaintiff Jasper Walker's expectation of confidentiality.

182. Plaintiff Jasper Walker has therefore had her privacy seriously invaded, her

biometric information non-consensually obtained, and been exposed to the risk and harmful conditions created by Otter's violations of Illinois law.

J. Plaintiff Michael Walker's Experience

183. Plaintiff Michael Walker participated in Zoom meetings while in Chicago, Illinois on January 10, 2025 and May 19, 2025 where the Otter Notetaker was used to transcribe the conversations that transpired therein, and during which Otter collected the biometric data and Speaker Data of the participants.

184. Plaintiff Michael Walker used Zoom to communicate with a financial professional, and thus, the call involved deeply personal and private financial information.

185. Plaintiff Michael Walker believes that the Otter Notetaker that appeared in the above-listed Zoom meetings was labeled something like "Michael's Notetaker," and after the meetings, Michael received emails from Otter indicating that the meetings had been recorded by Otter. Michael does not know why. To the best of his knowledge and memory, Michael has never signed up for an Otter account.

186. Plaintiff Michael Walker was not aware, nor did he have any reason to suspect that Otter would obtain and retain his biometric data and Speaker Data.

187. Nor was Plaintiff Michael Walker informed that Otter would use his communications to train its ASR and machine learning tools.

188. Through this process, Otter read and learned, in real time, the content of Plaintiff Michael Walker's communications.

189. Otter did not procure Plaintiff Michael Walker's prior consent, express or otherwise, to have Otter record and use his biometric data or Speaker Data. Nor did Plaintiff Michael Walker give his prior consent, express or otherwise, to Otter to allow Otter to intercept his biometric data or Speaker Data.

190. Further, Plaintiff Michael Walker never consented to Otter's use of his communications to train its ASR and machine learning systems or indefinitely store his private communications and Speaker Data and exploit them for commercial gain.

191. During the above-listed Zoom meetings, Otter captured Plaintiff Michael Walker's voiceprint and voiceprints of other attendees, and it created a transcript of the meetings using the same.

192. Otter did so without first informing Plaintiff Michael Walker that it was collecting his biometric data and without first obtaining, from him, a written release for the collection of that data.

193. Plaintiff Michael Walker neither granted nor would have granted Otter consent to obtain his biometric data or Speaker Data if he had been given the opportunity.

194. Plaintiff Michael Walker's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff Michael Walker's express and informed consent. The intrusion is especially troubling given the sensitive nature of the discussion and Plaintiff Michael Walker's expectation of confidentiality.

195. Plaintiff Michael Walker has therefore had his privacy seriously invaded, his biometric information non-consensually obtained, and been exposed to the risk and harmful conditions created by Otter's violations of Illinois law alleged below.

K. Plaintiff Winston's Experience

196. Plaintiff Winston participated in Zoom meetings while in Illinois during the applicable period governed by the statute of limitations, where the Otter Notetaker was used by a meeting participant to transcribe the conversations that transpired therein.

197. Plaintiff Winston used Zoom, Microsoft Teams, and other video conferencing platforms to communicate information related to her job—such as sensitive business discussions, strategic planning sessions, confidential project meetings, performance reviews, discussions with clients, internal team meetings, and other professional communications.

198. Thus, these Conversations involved professional communications which Plaintiff Winston reasonably expected would remain private among the invited

participants, and which Otter recorded, transcribed, and stored without her knowledge, permission, or consent.

199. Plaintiff Winston was not and is not an Otter accountholder.

200. Plaintiff Winston was not aware, nor did she have any reason to suspect that Otter, as opposed to the Otter accountholder, would obtain and retain her conversational data.

201. Nor was Plaintiff Winston informed that Otter would use her communications to train its ASR and machine learning tools.

202. Through this process, Otter read and learned, in real time, the content of Plaintiff Winston's communications.

203. Otter did not procure Plaintiff Winston's prior consent, express or otherwise, to have Otter eavesdrop, record, and use her communications and Speaker Data. Nor did Plaintiff Winston give her prior consent, express or otherwise, to Otter to allow Otter to wiretap her communications or intercept her Speaker Data.

204. Further, Plaintiff Winston never consented to Otter's use of her communications to train its ASR and machine learning systems or indefinitely store her private communications and Speaker Data and exploit them for commercial gain.

205. Plaintiff Winston neither granted nor would have granted Otter consent to record her conversation on Zoom or obtain her Speaker Data if she had been given the opportunity.

206. During the Conversations, Otter captured Plaintiff Winston's voiceprint and voiceprints of other attendees, and it created a transcript of the Conversations using the same.

207. Otter did so without first informing Plaintiff Winston that it was collecting her biometric data and without first obtaining, from her, a written release for the collection of that data.

208. Plaintiff Winston neither granted nor would have granted Otter consent to

record her Conversations on various meeting platforms or obtain her Speaker Data if she had been given the opportunity.

209. Plaintiff Winston's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff Winston's express and informed consent. The intrusion is especially troubling given the sensitive nature of the discussion and Plaintiff Winston's expectation of confidentiality.

210. Plaintiff Winston felt frustrated, embarrassed, and stressed to learn that her conversation was recorded without her consent, and her information, voice, and conversation content remains in Otter's possession indefinitely for Otter's commercial use and training of its machines/technology.

211. Plaintiff Winston has therefore had her privacy seriously invaded, her biometric information non-consensually obtained, and been exposed to the risk and harmful conditions created by Otter's violations of federal and Illinois law.

L. Plaintiff Dolan's Experience

212. Plaintiff Dolan participated in a Zoom meeting in Washington state in March 2024 where the Otter Notetaker recorded the call. Plaintiff Dolan had no reason to suspect that the conversation was being recorded.

213. Plaintiff Dolan used Zoom to communicate regarding certain professional opportunities, which Otter recorded, transcribed, and stored without his knowledge, permission, or consent.

214. To his knowledge, Plaintiff Dolan did not create an account with Otter.

215. Plaintiff Dolan was not aware, nor did he have any reason to suspect that Otter would obtain and retain his conversational data and Speaker Data.

216. Nor was Plaintiff Dolan informed that Otter would use his communications and Speaker Data to train its ASR and machine learning tools.

217. Through this process, Otter read and learned, in real time, the contents of Plaintiff Dolan's communications.

218. Otter did not procure Plaintiff Dolan's prior consent, express or otherwise, to have Otter eavesdrop, record, and use his communications and Speaker Data. Nor did Plaintiff Dolan give his prior consent, express or otherwise, to Otter to allow Otter to wiretap his communications or intercept his Speaker Data.

219. Further, Plaintiff Dolan never consented to Otter's use of his communications and Speaker Data to train its ASR and machine learning systems or indefinitely store his private communications and Speaker Data and exploit them for commercial gain.

220. Plaintiff Dolan neither granted nor would have granted Otter consent to record his conversation on Zoom or obtain his Speaker Data if he had been given the opportunity.

221. Plaintiff Dolan's conversational data and Speaker Data remain on Otter's servers, from which Otter continues to profit, despite never obtaining Plaintiff' Dolan's express and informed consent.

222. Plaintiff Dolan felt frustrated, embarrassed, and stressed to learn that his conversation was recorded without his consent, and his information, voice, and conversation content remains in Otter's possession indefinitely for Otter's commercial use and training of its machines/technology.

223. Plaintiff Dolan has, therefore, had his privacy severely invaded and been exposed to the risk and harmful conditions created by Otter's violations of federal and Washington law alleged below.

CLASS ACTION ALLEGATIONS

224. Under FED. R. CIV. P. 23(b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a nationwide class defined as follows (the "Nationwide Class"):

> All individuals whose conversations were recorded at least once by Otter who did not have an account with Otter at the time of recording, during the applicable statute of limitations.

225. Under FED. R. CIV. P. 23(b)(2), (b)(3), and (c)(4), Plaintiffs further seek

certification of a California subclass defined as follows (the "California Subclass"):

> All individuals whose conversations were recorded at least once by Otter while the individuals were in California and/or were participating in a meeting hosted in California, and who did not have an account with Otter at the time of recording, during the applicable statute of limitations.

226. Under FED. R. CIV. P. 23(b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of an Illinois subclass defined as follows (the "Illinois Subclass"):

> All individuals whose conversations were recorded at least once by Otter while the individuals were in Illinois and/or were participating in a meeting hosted in Illinois, during the five years preceding the filing of this action. Excluded from this definition are individuals who had Otter accounts at the time of recording.

227. Under Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a Washington subclass defined as follows (the "Washington Subclass"):

> All individuals whose conversations were recorded at least once by Otter while the individuals were in Washington and/or were participating in a meeting hosted in Washington, and who did not have an account with Otter at the time of recording, during the applicable statute of limitations.

228. The Nationwide Class, California Subclass, Illinois Subclass, and Washington Subclass shall be collectively referred to as the "Class."

229. Excluded from the Class are Otter's employees, officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; class counsel and their employees; and the judicial officers and their immediate family members and associated court staff assigned to this case.

230. **Numerosity**. The number of persons within the Class is substantial and believed to amount to thousands, if not millions, of persons. It is impractical to join each member of the Class as a named Plaintiff. Further, the size and modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly,

utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

231. **Commonality and Predominance.** This case presents questions of law and fact common to all Class members, which predominate over individualized issues. Those common questions include:

a. Whether Otter's practices violate the ECPA;

b. Whether Otter's practices violate the CFAA;

c. Whether Otter's practices violate CIPA;

d. Whether Otter's practices violate the CDAFA;

e. Whether Otter's practices violate California's prohibitions against intrusion upon seclusion and conversion;

f. Whether Otter's practices violate California's prohibition against larceny and the receipt of stolen property, Cal. Penal Code § 496(a) and (c);

g. Whether Otter's practices violate California's constitutional prohibition against invasion of privacy;

h. Whether Otter's practices violate the UCL;

i. Whether Otter's practices violate BIPA, Section 15(a) and 15(b);

j. Whether Otter sought or obtained consent—express or otherwise—from Plaintiffs and the Class prior to intercepting and recording their communications or obtaining their voiceprints;

k. Whether Otter's practices violate the Washington Wiretapping Law;

l. Whether Otter obtained consent to store and use Plaintiffs' and Class Members' voice prints, communications, and other data to train their AI systems;

m. Whether Plaintiffs and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations; and

n. Whether Otter should be enjoined from obtaining Plaintiffs' and Class

members' personal information and communications and be required to destroy all information obtained by virtue of the unlawful data collection.

232. **Typicality.** The claims of the named Plaintiffs are typical of the Class, because the named Plaintiffs, like all other Class members, had the content of their communications read, learned, analyzed, and/or examined by Otter, as well as their Speaker Data obtained by Otter.

233. **Adequacy of Class Representative.** Plaintiffs are adequate class representatives. They seek relief for all members of the Class and will put the interests of the Class ahead of their individual interests. Plaintiffs do not have conflicts of interest with any other member of the Class.

234. **Adequacy of Class Counsel.** Plaintiffs have retained experienced counsel who have successfully prosecuted class actions, including privacy class actions, in California courts, as well as in state and federal courts throughout the country.

235. **Superiority and Manageability.** Class-wide adjudication will produce substantial benefits for the Court and for litigants because joinder of all individual Class members is impracticable and inefficient, particularly when compared to the relatively small amount-in-controversy for most individual Class members. Moreover, the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications. As a result, class-wide adjudication presents fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

236. **Injunctive or Declaratory Relief**. Otter's acts or omissions giving rise to the invasion of the Plaintiffs' privacy are common to the class. Injunctive relief or declaratory relief that is proper for the Plaintiffs will be appropriate with respect to the Class as a whole.

TOLLING

237. The statutes of limitations applicable to Class claims were tolled by Otter's

conduct and Plaintiffs' and Class members' delayed discovery of their claims to the time when Otter began joining calls online, without permission.

238. As alleged above, Plaintiffs and the Class members did not know, and could not have known, the full extent of Otter's surreptitious gathering, storage, and monetizing of their private conversations without consent.

239. Plaintiffs and the Class members could not have discovered, through the exercise of reasonable diligence, the full scope of Otter's alleged unlawful conduct, as it not only recorded their private conversations and information without consent, but also stored and monetized it in a way that Plaintiffs and the Class members do not have control over. Additionally, on information and belief, Otter has already used this information for its commercial advantage by incorporating it into its AI training models.

240. Otter did not make clear to Plaintiffs and the Class members the full extent of its recording, storage, and monetization of their conversations, and continues to store and commercially benefit from this information, causing a continuing violation of Plaintiffs' and Class members' rights.

241. All applicable statutes of limitations have been tolled by operation of the delayed discovery rule. Under the circumstances, Otter was under a duty to disclose the nature and significance of the invasion of privacy but did not do so. Otter is therefore estopped from relying on any statute of limitations.

CAUSES OF ACTION

Count 1: Electronic Communications Privacy Act of 1986 18 U.S.C. § 2510, *et seq.* (*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

242. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

243. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Case Act of 1986, prohibits the intentional interception of the contents of any wire,

oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

244. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

245. Otter's actions in intercepting Plaintiffs' and Class members' oral communications while they participated in Google Meet, Zoom, and Microsoft Teams calls was intentional. Otter is aware that it is intercepting the communications of non-Otter accountholders in these circumstances and has taken no remedial action.

246. Otter's interceptions of Plaintiffs' and Class members' oral communications was done contemporaneously while those communications transpired.

247. The communications intercepted by Otter included the contents of the Google Meet, Zoom, and Microsoft Teams calls—i.e., the oral and conversational data contained therein.

248. The transmission of conversational data between Plaintiffs and the Class members on the one hand and the Otter Notetaker/OtterPilot on the other, without authorization, constituted "transfer[s] of signs, signals, writing . . . data [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system that affects interstate commerce[,] and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

249. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The Otter Notetaker and OtterPilot software;

b. Plaintiffs' and Class members' Google Meet, Zoom, Microsoft Teams, and other virtual meeting platforms;

c. Plaintiffs' and Class members' computing and mobile devices;

d. The servers from which Otter intercepted the Plaintiffs' and Class members' communications;

e. Any other tools used to intercept Plaintiffs' and Class members'

communications.

250. Otter was not an authorized party to the communications because Plaintiffs and Class members did not consent to Otter's transcription of their communications; were not aware that Otter itself was in the process of obtaining and retaining Plaintiffs and Class members' communications, including for the improvement of its ASR and machine learning models; and as a result, did not knowingly provide their communications to Otter, as opposed to Otter accountholders and other conversational participants.

251. Otter could not manufacture its own status as a party to Plaintiffs' and Class members' communications with others by deceptively and surreptitiously intercepting those communications.

252. Plaintiffs and the Class members did not consent to the interception of their communications, as they never had the opportunity to assent to the same.

253. Moreover, they could not have been said to have even impliedly consented to interception, as they were not fully informed of Otter's role as an active third-party listener and autonomous data harvesting agent, including the use of their data to train Otter's ASR and machine learning models. *Cf. Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014).

254. Hosts of meetings in which Plaintiffs participated did not properly consent to the illegal collection of data from other meeting participants to whom no notice or improper notice was given about the recording and/or transmission of data to Otter.

255. Further, by converting and then using conversational data from Plaintiffs and Class members—without their knowledge, consent, or compensation— to train its ASR and machine learning systems for its own pecuniary gain, Otter engaged in conduct with an unlawful and tortious purpose, supporting additional claims under, *inter alia*, the CFAA and CDAFA, as well as common law claims under California law for intrusion upon seclusion and conversion. Otter's tortious purpose falls within the "crime-tort" exception, thus, removing any statutory immunity Otter may otherwise claim under the ECPA.

256. After intercepting the communications, Otter then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

257. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and Class members; injunctive and declaratory relief, sufficient to prevent the same or similar conduct by Otter in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

258. Plaintiffs and the Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 2: Computer Fraud and Abuse Act
18 U.S.C. § 1030, *et seq.*
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

259. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

260. The CFAA, enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

261. The CFAA reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of information within their computers.

262. The CFAA provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

263. Further, the CFAA mandates that it is unlawful to "knowingly and with intent to defraud, access[] a protected computer without authorization or exceed[ing] authorized access" and thereby "further[] the intended fraud and obtain[] anything of value" 18 U.S.C. § 1030(a)(4).

264. Plaintiffs and Class members, as individuals, and Otter as a corporation or legal entity, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

265. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

266. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

267. Otter's use of the Otter Notetaker and OtterPilot constitute access to the Plaintiffs' and Class member's computers, including but not limited to, desktop computers, laptop computers, and mobile devices.

268. Through the Otter Notetaker and OtterPilot, Otter intentionally accessed Plaintiffs' and Class members' protected computers without their authorization or consent, or in a manner that exceeded Plaintiffs' and Class members' authorization and obtained information therefrom in contravention of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

269. Otter's misconduct constitutes a knowing intent to defraud Plaintiffs and the Class members of their personal data and to thereby derive financial gain. 18 U.S.C. § 1030(a)(4).

270. Plaintiffs and Class members have suffered harm and injury due to Otter's unauthorized access to the communications containing their private and personal information.

271. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Because the loss to Plaintiffs and Class members during any one-year period within the relevant timeframe, including the loss of their privacy interest in and control over their personal data, exceeded $5,000 in aggregate, Plaintiffs

and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

272. Plaintiffs and the Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 3: Intrusion Upon Seclusion
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

273. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

274. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

275. In carrying out its scheme to track and intercept Plaintiffs' and Class members' communications, Otter intentionally intruded upon Plaintiffs' and the Class members' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

276. Otter's interception, transcription, and use of Plaintiffs' and the California Class members' data were not authorized by Plaintiffs and the Class members.

277. Otter's intentional intrusion into Plaintiffs' and the Class members' communications and their computing devices was highly offensive to a reasonable person in that they violated federal and state laws designed to protect individual privacy and against theft.

278. The taking of private conversational data from consumers through deceit is highly offensive behavior, particularly where, as here, Plaintiffs and the California Class members were never given an adequate opportunity to opt-out from the interception of their data.

279. Wiretapping, surreptitious, and deceitful recording of communications for undisclosed motives is highly offensive behavior.

280. Plaintiffs and the Class members have been damaged by Otter's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful use of their communications for ASR training and machine learning.

281. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until Otter is enjoined, and restrained by order of this Court, Plaintiffs have no way of controlling their own information and ensuring that their personal conversations and data remain private or the recordings, screenshots, and transcripts in Otter's possession are destroyed. Furthermore, based on Otter's statements on its websites, it stores speaker data and information indefinitely, and without the Court's injunctive relief, there is no other way for Plaintiffs and the Class to prevent Otter from using their names, data, recorded conversations, and voice prints.

282. Without injunctive and declaratory relief, Otter will continue profiting from its illegally obtained data, and Plaintiffs and Class Members are at a heightened risk of this information being shared or stolen. Thus, Otter's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members, through its continued storage and use of the unlawfully collected information. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

283. Plaintiffs and the Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 4: Conversion
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

284. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set

forth herein.

285. Plaintiffs and the Class members have property interests in their personal conversational data, as well as aspects of their likeness, such as their Speaker Data.

286. Plaintiffs and the Class members at no time consented to Otter appropriating their conversational and Speaker Data for the purposes of transcription or for using the recordings and transcriptions produced to train Otter's ASR and machine learning systems.

287. Otter wrongfully disposed of Plaintiffs' and the Class members' property by causing conversational and Speaker Data to be transmitted between their computers and mobile devices and Otter using the Otter Notetaker and OtterPilot without their consent and without payment.

288. As a result of Otter's conversion, Plaintiffs and the Class members have suffered injury and damages in an amount to be proven at trial.

289. Plaintiffs and the Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 5: Unjust Enrichment
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

290. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

274. Through its unlawful, unfair and deceptive conduct, Otter knowingly obtained significant revenue from its unlawful collection and use of Plaintiffs' and Class Members' data by using and processing it for commercial gain, including improving its products.

275. By absconding and misusing Plaintiffs' and Class Members' personal data, Otter was unjustly enriched and received both financial and non-financial benefits. For example, Otter exploits illegally obtained conversations for its own commercial advantage

such as training its proprietary software, improving its services, contracting with service vendors, and more.

276. Otter enriched itself by saving the costs it reasonably should have spent by obtaining users consent to record and use their private communications. Yet, to increase profits, and at the expense of Plaintiffs and the Class, it gained a competitive and financial advantage by failing to obtain proper consent to record and use this information. Due to Otter's conduct, Plaintiffs and Class Members suffered harm, including from privacy invasion, loss of compensation/value for their data, and the lost profits from the use of their personal data.

277. It would be inequitable and unjust to permit Otter to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiffs and Class Members.

278. Otter will be unjustly enriched if it is permitted to retain the economic benefits conferred upon it by Plaintiffs and Class Members through its obtaining of their personal data and the value thereof, and profiting from the unlawful, unauthorized, and impermissible use of this data.

279. Plaintiffs and Class Members are therefore entitled to recover the amounts realized by Otter at their expense.

280. Since Plaintiffs and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Otter's ill-gotten gains, and/or other sums as may be just and equitable. In the absence of completed discovery regarding class certification and merits, forcing an election of remedies at the initial pleading stage is premature.

Count 6: Declaratory Judgment under 28 U.S.C. § 2201, et. seq.
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

281. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

282. The Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

283. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

284. An actual controversy has arisen as to whether Otter unlawfully collected certain information from Plaintiffs and the Class Members, and how Otter continues to use that information for its own financial gain, as well as whether Otter shares that information with third parties.

285. Plaintiffs and the Class Members are entitled to equitable relief as no adequate remedy at law exists.

a. Otter has not yet implemented adequate protections to protect Plaintiffs and Class Members' personal data or conversations, nor has it given adequate notice to all affected class members, leaving individuals potentially unsure if their conversations have been recorded and kept by Otter. Therefore, the equitable relief requested here would prevent ongoing and future harm to Plaintiffs and the Class Members. Since Otter still has Plaintiffs' and Class Members' information, without an

injunction, Plaintiffs and the Class Members cannot be sure that the information is secure and private or properly destroyed.

b. Injunctive relief is also necessary to protect members of general public from Otter's unlawful recording and storage of private conversations. Without court intervention, Otter will likely continue its privacy violations.

c. While Otter has disclosed how it may use Plaintiffs' and Class Members' private conversations and information, it is not currently known specifically what information is being kept, how it is being used, and when, if ever, it will be destroyed. Therefore, injunctive relief would ensure and provide Plaintiffs and the public with ability to control access to their information, and limit its exposure.

d. In addition, discovery—which has not yet been provided—may reveal that the claims providing legal remedies are inadequate. At this time, in the absence of completed discovery regarding class certification and merits, forcing an election of remedies at the initial pleadings stage is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

286. Plaintiffs and the Class Members therefore seek a declaration that Otter

violated their privacy and property rights, and Otter must take remedial measures, including, but not limited to:

a. Prohibiting Otter from engaging in the wrongful acts stated herein;

b. Requiring Otter to implement adequate security and privacy protocols and practices consistent with industry standards, applicable regulations, and federal, state, and local laws;

c. Mandating that Otter provide proper notice to all affected parties, and posted publicly;

d. Requiring that Otter delete, destroy, and purge Plaintiffs' and Class Members' unlawfully obtained data;

e. Requiring Otter to engage independent third-party auditors and/or internal personnel to ensure all unlawfully obtained information is permanently deleted and purged from its system; and,

f. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

Count 7: Trespass to Chattels
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, Winston, Dolan, and the Nationwide Class*)

287. Plaintiffs incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

288. Otter, intentionally and without consent or other legal justification, obtained the contents of Plaintiffs' and Class Members' private conversations and voiceprints by surreptitiously recording and storing their online meeting information without consent.

289. Otter placed the OtterPilot and OtterNotetaker into the online calls of Plaintiffs and Class Members, without their knowledge or consent, causing their private information and voiceprints to be recorded, stored, processed, and otherwise used to benefit Otter.

290. Otter additionally engineered a process in which Plaintiffs and Class Members would be notified of notes from a meeting (even though Plaintiffs had not consented to it) and in an attempt to access the notes that were taken in the meeting, Otter would then software installed on their computer to spread further despite Plaintiffs and Class Members not intending to do so.

291. Otters' intentional and unjustified interception of Plaintiffs' and Class Members' private communications and voiceprints as well as its intentional and misleading methods to spread its software interfered with Plaintiffs' and Class Members' use of the following personal property owned by Plaintiffs: (a) Plaintiffs' computers and phones; and (b) Plaintiffs' personally identifiable information.

Count 8: California Invasion of Privacy Act
Cal. Penal Code §§ 631 and 632
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

292. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

293. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose: "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

294. Cal. Penal Code § 631(a) provides that: "Any person who, by means of any

machine, instrument, or contrivance, or in any other manner…willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500)."

295. California Penal Code § 632(a) provides, in pertinent part: "A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . ."

296. At all relevant times, Otter intercepted, recorded, transcribed, and utilized Plaintiffs' and California Class members' communications exchanged with others using platforms such as Google Meet, Zoom, and Microsoft Teams, while those communications were in transit or passing over any wire, line, or cable or were being sent or received from any place in California.

297. As recounted above, Otter willfully and intentionally intercepted these communications without consent from all parties to the communications.

298. Otter intended to learn, and did learn, the meaning of the content in the communications it intercepted.

299. Otter's subsequent "de-identification" process reveals that Otter necessarily became aware of the content of the California Class members' communications as those

communications were transmitted to Otter in real-time.

300. Otter Notetaker and OtterPilot are "machine[s], instrument[s], contrivance[s], or . . . other manner[s]" used to engage in the prohibited conduct at issue here.

301. The following items additionally constitute "machine[s], instrument[s], contrivance[s], or . . . other manner[s]" within the meaning of CIPA:

a. The Plaintiffs' and California Class members' Google Meet, Zoom, Microsoft Teams, and other virtual meeting platforms.

b. The Plaintiffs' and California Class members' computing and mobile devices**.**

c. The servers from which Otter intercepted the Plaintiffs' and California Class members' communications.

d. Any other tools used to intercept the Plaintiffs' and California Class members' communications.

302. Otter is a separate legal entity that offers "'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021).

303. Accordingly, Otter was a third party to the Plaintiffs' and Class members' intercepted communications. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

304. Otter's interception of Plaintiffs' and California Class members' communications during their Google Meet, Zoom, Microsoft Teams, and other meetings originated in and transpired in California.

305. The data collected by Otter constituted "confidential communications" as that term is used in Section 632, because Plaintiffs and California Class members had objectively reasonable expectations of privacy while engaging in private conversations and calls using Google Meet, Zoom, and Microsoft Teams.

306. The violations of CIPA §§ 631 and 632 constitute an invasion of privacy

sufficient to confer Article III standing.

307. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and California Class Members have been injured by the violations of CIPA §§ 631 and 632, and each seeks the greater of $5,000 per violation or three times the actual amount of damages, as well as injunctive relief, for Otter's violations of CIPA §§ 631 and 632.

308. Plaintiffs and the California Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 9: California Invasion of Privacy Act
Cal. Penal Code § 635
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

309. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

310. CIPA § 635 makes punishable anyone "who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another[.]" Cal. Penal Code § 635.

311. The Otter Notetaker/OtterPilot is a "device" which is "designed or intended for eavesdropping upon the communication of another."

312. Injuries caused using Otter Notetaker/OtterPilot are traceable to Otter's furnishing and provision of the device.

313. Plaintiffs and California Class members are entitled to bring a CIPA § 635 claim per CIPA § 637.2. The court in *In re Meta Pixel Tax Filing Cases* noted that "[b]y including Section 635 within the provisions enforceable under Section 637.2 [] the California Legislature clearly intended to permit private enforcement[.]" 724 F. Supp. 3d 987, 1009 (N.D. Cal. 2024).

314. Plaintiffs and the California Class members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per

violation.

Count 10: California Invasion of Privacy Act
Cal. Penal Code § 638.51
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

315. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

316. CIPA § 638.51 provides that "a person may not install or use a pen register or a trap and trace device without first obtaining a court order[.]" Cal. Penal Code § 638.51.

317. A "pen register" is defined as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

318. A "trap and trace device" is defined as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

319. Courts interpret "trap and trace device" and "pen register" broadly. The court in *Greenley v. Kochava, Inc*. noted Section 638.50's "expansive language" and explained that this "indicates courts should focus less on the form of the data collector and more on the result." 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023). *See also Rodriguez v. Autotrader.com, Inc*., 762 F. Supp. 3d 921, 929 (C.D. Cal. 2025) (rejecting defendant's suggestion that Section 638.51 applies only to telephone surveillance, not software: "the definitions supplied by § 638.51 are not so limited").

320. Otter violated Section 638.51 by using software to record private communications without consent and then transfer it for its own use.

321. Otter did not obtain a court order to use the Otter Notetaker/OtterPilot to

record private communications.

322. Plaintiffs and the Class Members did not consent to the use of a pen register or trap and trace device.

323. Plaintiffs and the Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

Count 11: Comprehensive Computer Data and Fraud Access Act
Cal. Penal Code § 502, *et seq.*
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

324. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

325. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Plaintiffs' and California Class members' computers, including desktops, laptops, and smart phone devices are "computers" within the meaning of the statute.

326. Otter violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and California Class members' data.

327. Otter was unjustly enriched, by acquiring Plaintiffs' and California Class members' valuable personal information without permission and using that information for Otter's own financial benefit to improve its ASR and machine learning models. Plaintiffs and the California Class members retain a stake in the profits Otter earned from the use of their personal data because, under the circumstances, it is unjust for Otter to retain those profits.

328. Otter accessed, copied, took, analyzed, and used data from Plaintiffs and

California Class members' computers in and from the State of California, where Otter: (1) has its principal place of business; and (2) used servers that provided communication links between Plaintiffs and California Class members' computers and Otter, which allowed Otter to access and obtain Plaintiffs' and California Class members' data. Accordingly, Otter caused the access of Plaintiffs' and California Class members' computers from California, and is therefore deemed to have accessed Plaintiffs' and California Class members' computers in California.

329. As a direct and proximate result of Otter's unlawful conduct within the meaning of Cal. Penal Code § 502, Otter has caused loss to Plaintiffs and California Class members and has been unjustly enriched in an amount to be proven at trial.

330. Plaintiffs, on behalf of themselves and California Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

331. Plaintiffs and the California Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

332. Plaintiffs and the California Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 12: Larceny/Receipt of Stolen Property
Cal. Penal Code § 496(a) and (c)
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

333. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

334. Courts recognize that internet users have a property interest in their personal information and data, including the Speaker Data. *See Calhoun v. Google, LLC,* 526 F. Supp. 3d 605, at *21 (N.D. Cal. Mar. 17, 2021) (recognizing property interest in personal information and rejecting Google's argument that "the personal information that

Google allegedly stole is not property"); *In re Experian Data Breach Litigation,* 2016 U.S. Dist. LEXIS 184500, at *5 (C.D. Cal. Dec. 29, 2016) (loss of value of PII is a viable damages theory); *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 460 (D. Md. 2020) ("The growing trend across courts that have considered this issue is to recognize the lost property value of this [personal] information."); *Simona Opris v. Sincera,* 2022 U.S. Dist. LEXIS 94192, at *20 (E.D. Pa. 2022) (collecting cases).

335. Cal. Penal Code § 496(c) permits any person who has been injured by a violation of section 496(a) to recover three times the amount of actual damages, costs of suit and attorney's fees in a civil suit.

336. Cal. Penal Code § 496(a) creates an action against any person who (1) receives any property that has been stolen or obtained in any manner constituting theft, knowing the property to be stolen or obtained, or (2) conceals, sells, withholds, or aids in concealing or withholding any property from the owner, knowing the property to be so stolen or illegally obtained.

337. Under Cal. Penal Code § 1.07(a)(38), "person" means "an individual, corporation, or association." Thus, Otter is a person under § 496(a).

338. As set forth herein, the Plaintiffs' and California Class members' private conversational information and Speaker Data was stolen or obtained by theft, without limitation, under Cal. Penal Code § 484, by false or fraudulent representations or pretenses. At no point did Otter have Plaintiffs' and California Class members' consent to record and process their private communications or Speaker Data.

339. Otter meets the grounds for liability of § 496(a) because it received information that was stolen or obtained by theft and/or false pretenses, and which it knew was obtained illegally when it received it.

340. As a direct and proximate result of the acts and omissions described above, Plaintiffs and the California Class members were injured by Otter's violations of section 496(a).

341. Pursuant to Cal. Penal Code § 496(c), Plaintiffs and the California Class members seek actual damages, treble damages, costs of suit, reasonable attorneys' fees, and any other damages that are authorized by law.

Count 13: Invasion of Privacy Under California Constitution
Cal. Const. Art. I, § 1
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

342. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

343. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I, § 1.

344. The right to privacy in California's Constitution creates a private right of action against private and government entities.

345. Plaintiffs and California Class members have and continue to have a reasonable expectation of privacy and interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications; and (2) being able to communicate without observation, intrusion or interference.

346. At all relevant times, by using the Otter Notetaker/Pilot to record and communicate Plaintiffs' and California Class members' private communications, Otter invaded their privacy rights under the California Constitution.

347. Plaintiffs and California Class members had a reasonable expectation that their communications would remain confidential, and that Otter would not secretly record their private conversations and then use them for their own commercial benefit, as well as share them with third parties.

348. This invasion of privacy is serious in nature, scope, and impact because it relates to communications that Plaintiffs and the California Class members intended to

keep private. Moreover, it constitutes an egregious breach of the societal norms underlying privacy rights.

349. As a result of Otter's actions, Plaintiffs and California Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

350. Plaintiffs and California Class members have been harmed as a direct and proximate result of Otter's invasion of their privacy and are entitled to injunctive relief.

351. Plaintiffs and the California Class members seek all other relief as the Court may deem just, proper, and available for invasion of privacy under the California Constitution.

Count 14: California Unfair Competition Law
Cal. Bus. Prof. Code § 17200 *et seq.*
(*On Behalf of Plaintiffs Brewer, Theus, Ryan, and the California Subclass*)

352. Plaintiffs Brewer, Theus, and Ryan (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

353. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200. By engaging in the aforementioned practices, Otter has violated the UCL.

354. Otter's "unlawful" acts and practices include its violations of the ECPA, CFAA, CIPA, CDAFA, Cal. Penal Code § 496(a) and (c), intrusion upon seclusion, conversion, and the California Constitution's prohibition against invasion of privacy.

355. Otter's conduct violated the spirit and letter of these laws, which protect property, economic and privacy interests, and prohibit the unauthorized interception and collection of private communications and information.

356. Otter's "unfair" practices include its violation of property, economic and privacy interests protected by the statutes and common law causes of action identified in paragraph 128. To establish liability under the unfair prong, Plaintiffs and the California Class members need not establish that these provisions were violated, although the claims

pleaded herein do.

357. Plaintiffs and California Class members have suffered an injury-in-fact, including the loss of money and/or property because of Otter's unfair and/or unlawful practices, to wit, the unauthorized disclosure and taking of their personal information, conversational data, and Speaker Data which has value as demonstrated by its use and value in training Otter's ASR and machine learning systems.

358. Otter's actions caused damage to and loss of Plaintiffs' and California Class members' property right to control the dissemination and use of their personal information, communications, and Speaker Data.

359. Plaintiffs and California Class members have suffered harm, not only in the form of diminution of the value of their private and personally identifiable data and content, but also harm for which there is no adequate legal remedy.

360. Damages cannot return the conversational data that Otter now has at its disposal for its ASR and machine learning purposes, and in turn, a legal remedy is inadequate to ensure the current protection and safety of Plaintiffs' and California Class members' conversational and Speaker Data, as well as the protection and safety of such data going forward. Accordingly, Plaintiffs and Class members seek equitable and injunctive relief, including but not limited to, deletion of the data Otter has unlawfully obtained.

361. Furthermore, as part of Otter's request for equitable relief, Otter seeks the restitution and disgorgement of unjust profits and revenues Otter reaped from using Plaintiffs' and California Class members' conversational and Speaker Data to improve its ASR and machine learning systems.

362. Plaintiffs and the California Class members also seek such other relief as the Court may deem equitable, legal, and proper.

Count 15: Illinois Biometric Information Privacy Act
740 ILCS 14/15(a)

(*On Behalf of Plaintiffs Jasper Walker, Michael Walker, Winston, and the Illinois Subclass*)

363. Plaintiffs Jasper Walker, Michael Walker, and Winston (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as if fully set forth herein.

364. Otter is a "private entity" as defined by BIPA. 740 ILCS 14/10.

365. Plaintiffs' and the Illinois Subclass's Speaker Data (defined above) qualify as "biometric identifier[s]" or "biometric information" as defined by BIPA. *Id.*

366. Otter violated BIPA by collecting and possessing Plaintiffs' and the Illinois Subclass's Speaker Data without first publishing a "written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS § 14/15(a).

367. As a result, Plaintiffs and members of the Illinois Subclass each seek and are entitled to (1) liquidated damages of $1,000 for each of Otter's negligent violations; (2) liquidated damages of $5,000 for each of Otter's reckless or intentional violations; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; (4) injunctive relief; and (5) any other relief that the Court deems appropriate. *Id.* § 14/20.

Count 16: Illinois Biometric Information Privacy Act
740 ILCS 14/15(b)
(*On Behalf of Plaintiffs Jasper Walker, Michael Walker, Winston, and the Illinois Subclass*)

368. Plaintiffs Jasper Walker, Michael Walker, and Winston (herein, "Plaintiffs") incorporate by reference paragraphs 1 through 241 as is fully set forth herein.

369. Otter is a "private entity" as defined by BIPA. 740 ILCS 14/10.

370. Plaintiffs' and the Illinois Subclass's Speaker Data qualify as "biometric

identifier[s]" or "biometric information" as defined by BIPA. *Id.*

371. Otter violated BIPA by collecting and possessing Plaintiffs' and the Illinois Subclass's Speaker Data without first: informing them in writing that a biometric identifier or biometric information was being collected or stored; informing them in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used; or obtaining a written release from them regarding the collection and storage of their biometric data. *Id.* § 14/15(b).

372. As a result, Plaintiffs and members of the Illinois Subclass each seek and are entitled to (1) liquidated damages of $1,000 for each of Defendant's negligent violations; (2) liquidated damages of $5,000 for each of Defendant's reckless or intentional violations; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; (4) injunctive relief; and (5) any other relief that the Court deems appropriate. *Id.* § 14/20.

Count 17: Washington Wiretapping Law
Wash. Rev. Code §§ 9.73.030, *et seq*.
(*On Behalf of Plaintiff Dolan and the Washington Subclass*)

373. Plaintiff Riley Dolan (herein, "Plaintiff Dolan") incorporates by reference paragraphs 1 through 241 as if fully set forth herein.

374. Washington law prohibits the interception or recording of a private phone call, in-person conversation, or electronic communication, unless all parties to the communication consent. Wash. Rev. Code § 9.73.030.

375. More specifically, the statute states that: "Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication." The same consent requirement applies to "private conversations

by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated."

376. Otter recorded private communications and/or conversation through the use of "devices," including the Otter Notetaker/OtterPilot, within the State of Washington.

377. Plaintiff Dolan and the Washington Subclass participated in online meetings where the Otter Notetaker/OtterPilot was enabled without their consent, meetings in which there was a justified expectation that their communications would not be intercepted.

378. Otter, using the Otter Notetaker/OtterPilot, intercepted and recorded the private communications of Plaintiff Dolan and the Washington Subclass in real time.

379. Otter then used the communications it intercepted to train its ASR and machine learning models—in other words, for its own financial benefit.

380. Plaintiff Dolan and the Washington Subclass did not consent to Otter's interception and use of their communications.

381. Otter's interception and use of Plaintiff Dolan's and Washington Subclass's communications was intentional, as Otter knowingly created and configured the Otter Notetaker/OtterPilot to intentionally intercept communications in Washington without consent from all the parties to the communication.

382. Plaintiff Dolan and Washington Subclass members were not aware that their electronic communications were being intercepted by Otter, nor did they ever consent to the same.

383. The plan to effectuate this tracking and interception of Plaintiff Dolan's and Washington Subclass members' communications while they were using Google Meet, Zoom, or Microsoft Teams was executed in Washington.

384. Defendant, knowing that this conduct was unlawful and a violation of Plaintiff Dolan's and the members of the Washington Subclass's right to privacy and a violation of Wash. Rev. Code § 9.73.030, *et seq*., did intrude on Plaintiff Dolan and the

members of the Washington Subclass's privacy by knowingly and/or negligently and/or intentionally engaging in the aforementioned recording activities relative to the conversations between Plaintiff Dolan and members of the Washington Subclass, on the one hand, and Otter on the other hand, as alleged herein above.

385. Based on the foregoing, Plaintiff Dolan and the members of the Washington Subclass are entitled to, and below herein do pray for, their statutory remedies and damages, including but not limited to, those set forth in Wash. Rev. Code § 9.73.060.

386. Pursuant to Wash. Rev. Code § 9.73.060, Plaintiff and the Washington Subclass seek (i) actual damages, not less than liquidated damages computed at the rate of $100 a day for each day of violation, not to exceed $1,000, and (ii) reasonable attorneys' fees and other costs of litigation incurred.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all others similarly situated, respectfully request:

a. certification of the proposed Class and Subclasses;

b. appointment of Plaintiffs' counsel as class counsel;

c. actual and statutory damages in an amount to be determined at trial;

d. a declaration that Otter's conduct was wrongful, unfair, unconscionable and in violation of federal, California, Illinois, and Washington law;

e. an order enjoining Otter's unlawful and unfair conduct;

f. restitution and disgorgement of all profits Otter wrongfully obtained;

g. an award to Plaintiffs and the Class of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law; and

h. such other relief as this Court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all applicable claims.

Respectfully submitted,

LEVIN LAW, P.A.
By: */s/ Brian Levin*
Brian Levin (*admitted by PHV*)
brian@levinlawpa.com
Brandon T. Grzandziel (*pro hac vice* to be filed)
brandon@levinlawpa.com
2665 South Bayshore Drive, PH2B
Miami, Florida 33133
Telephone 305-539-0593
Jacob Polin (SBN 311203)
jacob@levinlawpa.com
344 20th Street
Oakland, CA 94612
Telephone: (305) 402-9050

CLARKSON LAW FIRM, P.C.
By: */s/ Yana Hart*
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

WERMAN SALAS P.C.
By: *Douglas M. Werman*
Douglas M. Werman (*admitted by PHV*)
dwerman@flsalaw.com
John J. Frawley (*admitted by PHV*)
jfrawley@flsalaw.com
Anne R. Kramer
akramer@flsalaw.com
77 W. Washington St., Suite 1402
Chicago, Illinois 60602

Telephone: (312) 419-1008

MEYER WILSON WERNING CO., LPA
By: *Matthew R. Wilson*
Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Jared W. Connors (*admitted by PHV*)
jconnors@meyerwilson.com
Ryne E. Tipton (*admitted by PHV*)
rtipton@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

ALMEIDA LAW GROUP LLC
By: *David S. Almeida*
David S. Almeida *(admitted by PHV)*
david@almeidalawgroup.com
849 W. Webster Avenue
Chicago, Illinois 60614
Tel.: (708) 437-6476

Attorneys for Plaintiffs & the Proposed Classes